Some Notes on the FFT

To do a 2^k FFT mod a prime p you need to choose a prime p whose remainders include 2^k-th roots of unity, and you need to find one such root that is not a 2^{k-1}-th root of unity,

This can be done by taking the 2^{k-1}-st powers mod p of the first few integers until you find one such that this power is p-1. Get this power by successive squaring, and to be safe mod on each squaring.

You then want to set up your spreadsheet without dollar signs, so you can copy it freely

We describe a possible set up for this, for k=3 here, so that there are 8 input coefficients of our polynomial which we enter in opposite to the normal order. Thus to describe the number 12345678 which is written say, as the polynomial as $78+56*100+ 34*100^2 +12*100^3$ with coefficients in the order 78 56 34 12 0 0 0 0.

I would do this rather inefficiently in space, by putting three rows of the modulus on the top, with three rows that give the appropriate powers of the 8^{th} root of unity where they belong.

Then underneath that I would put the input and then put the three rows that do the FFT.

The first row has to be entered in your favorite way. The rest of the rows can be obtained entirely by copying the first row judiciously/

How?
Suppose you have the first row of the FFT let your data be denoted as
d0 d1 d2 d3 d4 d5 d6 d7
then the first row has the following entries (leaving out the mods and with x your 16^{th} root of unity)
d0+d4 d0-d4 d1+d5 (d1-d5)*x d2+d6 (d2-d6)*x^2 d3+d7 (d3-d7)*x^3

(where you have multiplier rows above that look like
1 1 1 x 1 x^2 1 x^3
1 1 1 1 1 x^2 1 x^2
1 1 1 1 1 1 1 1
and multiply the appropriate combinations of the row above by the multiplier in these rows above.

Then to form the second row, you copy the first and fourth and fifth and 8^{th} entrees here down, and copy the first and fifth to the right into the second and sixth places and the fourth and eighth to the left into the third and seventh places.
To form the third row you take the first and eighth and copy them down, and then copy the first to the right into the next three places, and the eighth to the left into the next three spaces.
A spreadsheet where this is done explicitly with formulae follows.
Here is the spreadsheet:

		power	0	1	2	3	4	5	6	7	
		modulus	**17**	17	17	17	17	17	17	17	
modulus	**17**	modulus	**17**	17	17	17	17	17	17	17	
8th root of 1	**2**	modulus	**17**	17	17	17	17	17	17	17	
inv of 8	**15**	multiplier	1	1	1	2	1	4	1	8	
		multiplier	1	1	1	1	1	1	4	4	
		multiplier	1	1	1	1	1	1	1	1	
		data	**78**	**56**	**11**	**12**	**0**	**0**	**0**	**0**	
		data modm	10	5	11	12	0	0	0	0	
		1st round	10	10	5	10	11	10	12	11	
		2nd round	4	3	16	0	0	4	6	13	
		3rd round=answer	4	7	5	13	4	16	10	4	

to invert FFT

		power	0	1	2	3	4	5	6	7	
		modulus	**17**	17	17	17	17	17	17	17	
modulus	17	modulus	**17**	17	17	17	17	17	17	17	
8th root of 1	2	modulus	**17**	17	17	17	17	17	17	17	
inv of 8	15	multiplier	1	1	1	2	1	4	1	8	
		multiplier	1	1	1	1	1	1	4	4	
		multiplier	1	1	1	1	1	1	1	1	
		data	**4**	**7**	**5**	**13**	**4**	**16**	**10**	**4**	
		data modm	4	7	5	13	4	16	10	4	
		1st round	8	0	6	16	15	14	0	4	
		2nd round	6	14	10	3	6	3	7	14	
		3rd round=answer	12	0	0	0	0	11	3	6	
	*	div by 8	10	0	0	0	0	12	11	5	10
		inv of 8	15	15	15	15	15	15	15	15	

Notice result on next to last line is input data backwards (last entry is a copy of the 1st

Here is what it looks like with formulae: (showingleft side first:

		power	0	=D1+1	=E1+1
		modulus	**=B3**	=D2	=E2
modulus	**17**	modulus	**=D2**	=D3	=E3
8th root of 1	**2**	modulus	**=D3**	=D4	=E4
inv of 8	**15**	multiplier	1	1	1
		multiplier	1	1	1
		multiplier	1	1	1
		data	**78**	**56**	**11**
		data modm	=MOD(D8,D4)	=MOD(E8,E4)	=MOD(F8,F4)
		1st round	=MOD(D9+H9,D2)	=MOD((D9-H9)*E5,E2)	=MOD(E9+I9,E2)
		2nd round	=MOD(D10+H10,D3)	=MOD(E10+I10,E3)	=MOD((D10-H10)*F6,F3)
		3rd round=answer	=MOD(D11+H11,D4)	=MOD(E11+I11,E4)	=MOD(F11+J11,F4)

A	B	C	D	E	F
			to invert FFT		

		power	0	=D16+1	=E16+1
		modulus	**=B18**	=D17	=E17
modulus	17	modulus	**=D17**	=D18	=E18
8th root of 1	2	modulus	**=D18**	=D19	=E19
inv of 8	15	multiplier	1	1	1
		multiplier	1	1	1
		multiplier	1	1	1
		data	**=D12**	**=E12**	**=F12**
		data modm	=MOD(D23,D19)	=MOD(E23,E19)	=MOD(F23,F19)
		1st round	=MOD(D24+H24,D17)	=MOD((D24-H24)*E20,E17)	=MOD(E24+I24,E17)
		2nd round	=MOD(D25+H25,D18)	=MOD(E25+I25,E18)	=MOD((D25-H25)*F21,F18)
		3rd round=answer	=MOD(D26+H26,D19)	=MOD(E26+I26,E19)	=MOD(F26+J26,F19)
		div by 8	=MOD(D27*D29,D17)	=MOD(E27*E29,E17)	=MOD(F27*F29,F17)
		inv of 8	=B20	=D29	=E29

:

=F1+1	=G1+1	=H1+1	=I1+1	=J1+1	1
=F2	=G2	=H2	=I2	=J2	2
=F3	=G3	=H3	=I3	=J3	3
=F4	=G4	=H4	=I4	=J4	4
=B4	1	=MOD(G5*G5,I2)	1	=MOD(I5*G5,K2)	5
1	1	1	=I5	=J6	6
1	1	1	1	1	7
12	**0**	**0**	**0**	**0**	8
=MOD(G8,G4)	=MOD(H8,H4)	=MOD(I8,I4)	=MOD(J8,J4)	=MOD(K8,K4)	9
=MOD((E9-I9)*G5,G2)	=MOD(F9+J9,F2)	=MOD((F9-J9)*I5,I2)	=MOD(G9+K9,G2)	=MOD((G9-K9)*K5,K2)	1
=MOD((E10-I10)*G6,G3)	=MOD(F10+J10,F3)	=MOD(G10+K10,G3)	=MOD((F10-J10)*J6,J3)	=MOD((G10-K10)*K6,K3)	1
=MOD(G11+K11,G4)	=MOD((D11-H11)*H7,H4)	=MOD((E11-I11)*I7,I4)	=MOD((F11-J11)*J7,J4)	=MOD((G11-K11)*K7,K4)	1
					1
					1
					1
=F16+1	=G16+1	=H16+1	=I16+1	=J16+1	1
=F17	=G17	=H17	=I17	=J17	1
=F18	=G18	=H18	=I18	=J18	1
=F19	=G19	=H19	=I19	=J19	1
=B19	1	=MOD(G20*G20,I17)	1	=MOD(I20*G20,K17)	2
1	1	1	=I20	=J21	2
1	1	1	1	1	2
=G12	**=H12**	**=I12**	**=J12**	**=K12**	2
=MOD(G23,G19)	=MOD(H23,H19)	=MOD(I23,I19)	=MOD(J23,J19)	=MOD(K23,K19)	2
=MOD((E24-I24)*G20,G17)	=MOD(F24+J24,F17)	=MOD((F24-J24)*I20,I17)	=MOD(G24+K24,G17)	=MOD((G24-K24)*K20,K17)	2
=MOD((E25-I25)*G21,G18)	=MOD(F25+J25,F18)	=MOD(G25+K25,G18)	=MOD((F25-J25)*J21,J18)	=MOD((G25-K25)*K21,K18)	2
=MOD(G26+K26,G19)	=MOD((D26-H26)*H22,H19)	=MOD((E26-I26)*I22,I19)	=MOD((F26-J26)*J22,J19)	=MOD((G26-K26)*K22,K19)	2
=MOD(G27*G29,G17)	=MOD(H27*H29,H17)	=MOD(I27*I29,I17)	=MOD(J27*J29,J17)	=MOD(K27*K29,K17)	=
=F29	=G29	=H29	=I29	=J29	2